UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/657,091	09/09/2003	Hiroyuki Tsuji	11-182	9837

23400 7590 12/27/2005

POSZ LAW GROUP, PLC
12040 SOUTH LAKES DRIVE
SUITE 101
RESTON, VA 20191

EXAMINER	
AU, SCOTT D	

ART UNIT	PAPER NUMBER
2635	

DATE MAILED: 12/27/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/657,091	TSUJI ET AL.	
	Examiner	Art Unit	
	Scott Au	2635	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *30 September 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-12* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-12* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.

5)☐ Notice of Informal Patent Application (PTO-152)

6)☐ Other: _____.

DETAILED ACTION

This communication is in response to applicant's response to an Amendment, which is filed September 30, 2005

An amendment to the claims 1-12 have been entered and made of record in the Application of Tsuji et al. for a "Remote control system" filed September 9, 2003.

Claims 1-12 are pending.

Response to Arguments

Applicant's arguments with respect to claims 1-12 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 1-4 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Regarding claims 1 and 3, the phrase "**in a case in**" renders the claim indefinite because it is unclear whether the limitation(s) following the phrase are part of the claimed invention. See MPEP § 2173.05(d).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-2 and 5-12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nakano (US# 6,181,252) in view of Gurney et al. (US# 5,905,445).

Referring to claim 1, Nakano discloses a remote control system comprising (i.e. see Figure 1): a transmitter (1) (i.e. transmitter) including enciphering means (11) (i.e. microprocessor) for enciphering a predetermined code through the use of a specific key code peculiar to each system, said transmitter (1) (i.e. transmitter) transmitting the enciphered code produced by said enciphering means (col. 2 lines 29-56); and a receiver (2) (i.e. receiver) including deciphering means (21) (i.e. microprocessor) for receiving the enciphered code to decipher the enciphered code through the use of said specific key code (i.e. key code), said receiver (2) (i.e. receiver) outputting an instruction for activating a controlled object (i.e. doors, trunk) when the deciphered code from said deciphering means satisfies a predetermined relationship (col. 2 line 58 to col. 3 line 17; see Figures 1-3).

However, Nakano did not explicitly disclose wherein, in a case in which said specific key code to be used in said deciphering means is transmitted from said

transmitter to said receiver and registered therein, said enciphering means enciphers said specific key code through the use of a default key code stored in said transmitter and said receiver, and said transmitter transmits the enciphered specific key code to said receiver.

In the same field of endeavor of vehicle security system, Gurney et al. disclose specific key code to be used in said deciphering means is transmitted from said transmitter to said receiver and registered therein, said enciphering means (20) (i.e. microprocessor) enciphers said specific key code through the use of a default key code (i.e. seed code) stored in said transmitter and said receiver, and said transmitter transmits the enciphered specific key code to said receiver (i.e. See Abstract, col. 1 line 49 to col. 2 line 10; see Figures 2 and 5).

One ordinary skill in the art understands that the algorithm generates the authenticator as a function of both the seed code and the function code of Gurney et al. is desirable in the vehicle security system of Nakano because Nakano suggests the receiver is constructed for demodulating the signal from the transmitter for actuating the door locking/unlocking, trunk, opening/closing, seat position adjusting and the like (col. 3 lines 1-17) and Gurney et al. suggest an algorithm in the transmitter and in the receiver has a cryptographic key and a seed code. Each algorithm generates the authenticator as a function of both the seed code and the function code; if the authenticators are equal, the message is valid. Upon each transmission the seed code is updated and the sequence number is incremented. The receiver updates its seed code according to the transmitted sequence number to keep the algorithm in

synchronism. Upon manufacture the transmitter sends the initial seed code and key to the receiver to program the receiver (i.e. see Abstract). Therefore, it would have been obvious to a person of ordinary skill in the art at the time of the invention was made to include the algorithm generates the authenticator as a function of both the seed code and the function code of Gurney et al. in the vehicle security system of Nakano with the motivation for doing so would allow the system highly secured.

Referring to claim 2, Nakano in view of Gurney et al. disclose the system according to claim 1, Nakano disclose wherein said transmitter (1) (i.e. transmitter) transmits the enciphered specific key code to said receiver when a predetermined operation is conducted (col. 2 lines 33-45).

Referring to claims 5 and 9, Nakano discloses a remote control system comprising (i.e. see Figure 1): a transmitter (1) (i.e. transmitter) including enciphering means (11) (i.e. microprocessor) having an enciphering table (i.e. see Figure 3) with a plurality of common key codes to be used for enciphering a specific key code specific to a particular remote control system (col. 2 line 29 to col. 3 line 30; see Figure 1-3).

However, Nakano did not explicitly disclose said enciphering means changing one of said plurality of common key codes to a registration key code set in advance to change the contents of said enciphering table and enciphering said specific key code through the use of the changed enciphering table including said registration key code, and said portable transmitter transmitting the enciphered specific key code produced by said enciphering means; and a receiver for outputting an instruction for activating a

controlled object (i.e. doors, trunk), said receiver including deciphering means for receiving the enciphered predetermined code to decipher the enciphered specific key code through the use of said registration key code stored in advance, said receiver registering the deciphered specific key code therein.

In the same field of endeavor of vehicle security system, Gurney et al. disclose enciphering means (14) (i.e. microprocessor) changing one of said plurality of common key codes to a registration key code set (i.e. seed codes) in advance to change the contents of said enciphering table and enciphering said specific key code through the use of the changed enciphering table including said registration key code (i.e. seed codes), and said transmitter (10) (i.e. fob) transmitting the enciphered specific key code produced by said enciphering means (14) (i.e. microprocessor); and a receiver (i.e. device within the vehicle) for outputting an instruction for activating a controlled object (i.e. doors, trunk, and seat adjust), said receiver including deciphering means (20) (i.e. microprocessor) for receiving the enciphered predetermined code to decipher the enciphered specific key code through the use of said registration key code (i.e. seed code) stored in advance, said receiver registering the deciphered specific key code therein (i.e. See Abstract, col. 1 line 49 to col. 2 line 10; see Figures 2 and 5).

One ordinary skill in the art understands that the algorithm generates the authenticator as a function of both the seed code and the function code of Gurney et al. is desirable in the vehicle security system of Nakano because Nakano suggests the receiver is constructed for demodulating the signal from the transmitter for actuating the door locking/unlocking, trunk, opening/closing, seat position adjusting and the like

(col. 3 lines 1-17) and Gurney et al. suggest an algorithm in the transmitter and in the receiver has a cryptographic key and a seed code. Each algorithm generates the authenticator as a function of both the seed code and the function code; if the authenticators are equal, the message is valid. Upon each transmission the seed code is updated and the sequence number is incremented. The receiver updates its seed code according to the transmitted sequence number to keep the algorithm in synchronism. Upon manufacture the transmitter sends the initial seed code and key to the receiver to program the receiver (i.e. see Abstract). Therefore, it would have been obvious to a person of ordinary skill in the art at the time of the invention was made to include the algorithm generates the authenticator as a function of both the seed code and the function code of Gurney et al. in the vehicle security system of Nakano with the motivation for doing so would allow the system highly secured.

Referring to claims 6 and 10, Nakano in view of Gurney et al. disclose the system according to claims 5 and 9, Nakano discloses a predetermined operation is conducted with respect to said portable transmitter (1) (i.e. transmitter), said transmitter (1) (i.e. transmitter) transmits the enciphered specific key code (col. 2 lines 33-57).

Referring to claims 7 and 11, Nakano in view of Gurney et al. disclose the system according to claims 5 and 9, Gurney et al. disclose wherein said enciphering means enciphers a predetermined code including said specific key code, said portable transmitter transmits the enciphered predetermined code to said receiver, said

deciphering means deciphers the enciphered predetermined code, and said receiver makes a decision as to whether or not the deciphered predetermined code is in a predetermined range with respect to a code stored in advance and, if the deciphered predetermined code is in said predetermined range, outputs said instruction for activating said controlled object (i.e. See Abstract, col. 1 line 49 to col. 2 line 10; see Figures 2 and 5).

Referring to claims 8 and 12, Nakano in view of Gurney et al. disclose the system according to claims 5 and 9, Gurney et al. disclose wherein the one of said plurality of common key codes is changed to said registration key code by said enciphering means for enciphering said specific key code (i.e. See Abstract, col. 1 line 49 to col. 2 line 10; see Figures 2 and 5).

Claims 3-4 are rejected under 35 U.S.C. 103(a) as being unpatentable over Brinkmeyer et al. (US# 5,596,317) in view of Gurney et al. (US# 5,905,445).

Referring to claim 3, Brinkmeyer et al. disclose a remote control system (i.e. see Figure available) comprising: a portable unit (20) (i.e. portable key) including enciphering means (21) (i.e. encoder) for enciphering a predetermined code through the use of a specific key code peculiar (i.e. Z', specific code transmitted from the vehicle to the portable device 20) to each system (G1-Gn) (i.e. vehicle functions of control devices), said portable unit (20) (i.e. portable key) transmitting the enciphered

code produced by said enciphering means (21) (i.e. encoder), and a vehicle-mounted control unit (Gi) (i.e. vehicle control device) including deciphering means(13) (decoder) for transmitting said predetermined code to said portable unit (20) (i.e. portable key) and receiving said enciphered code returned from said portable unit (20) (i.e. portable key) in response to the transmission of said predetermined code to decipher the enciphered code through the use of said specific key code (col. 5 lines 3-12), said vehicle-mounted control unit (Gi) (i.e. vehicle control device) outputting an instruction for activating a controlled object when the deciphered code produced by said deciphering means (13) (decoder) satisfies a predetermined relationship with respect to the transmitted predetermined code (col. 5 lines 25-43; see Figure available).

However, Brinkmeyer et al. did not explicitly disclose wherein, in a case in which said specific key code to be used in said deciphering means is transmitted from said portable unit to said vehicle-mounted control unit and registered therein, said enciphering means enciphers said specific key code through the use of a default key code stored in said portable unit and said vehicle-mounted control unit, and said portable unit transmits the enciphered specific key code to said vehicle-mounted control unit.

In the same field of endeavor of vehicle security system, Gurney et al. disclose said specific key code to be used in said deciphering means is transmitted from said portable unit (10) (i.e. fob) to said vehicle-mounted control unit (i.e. unit with the vehicle 18, see figure 1) and registered therein, said enciphering means enciphers said specific key code through the use of a default key code (i.e. seed code) stored in said

portable unit (10) (i.e. fob) and said vehicle-mounted control unit, and said portable unit (10) (i.e. fob) transmits the enciphered specific key code to said vehicle-mounted control unit (i.e. See Abstract, col. 1 line 49 to col. 2 line 10; see Figures 2 and 5).

One ordinary skill in the art understands that the algorithm generates the authenticator as a function of both the seed code and the function code of Gurney et al. is desirable in the vehicle security system of Brinkmeyer et al. because Brinkmeyer et al. disclose the electronic key (20), random number information (Z') transmitted from the vehicle is received by receiver (22) and passed on to encoder (21), which contains both the coding algorithm signal and the secret information of the safety device. By means of the coding algorithm, user code information (C'') is generated from the received signal that contains the random number information (Z'') in encoded form as well as additional code information (e.g. concerning the identity of electronic key (20)). This user code information (C'') is sent from encoder (21) to transmitter (23) of electronic key (20), which transmits it to the vehicle. User code information (C') received by the vehicle through its receiver (5) is delivered by the latter to CAN-bus (2), and thence to each of the individual control devices (G.sub.1 to G.sub.n), where it is fed to a decoder (13) which recovers the encoded information therefrom and checks the key identification code part to makes sure that the supply code signal was generated by an authorized key (20). If this check is positive, the control devices (G.sub.1 to G.sub.n) extract from the user code information (C') the random number information (Z') contained therein, and supply it to another downstream comparator (15) (col. 5 lines 3-43) and Gurney et al. suggest an alternative of algorithm in the

transmitter and in the receiver has a cryptographic key and a seed code. Each algorithm generates the authenticator as a function of both the seed code and the function code; if the authenticators are equal, the message is valid. Upon each transmission the seed code is updated and the sequence number is incremented. The receiver updates its seed code according to the transmitted sequence number to keep the algorithm in synchronism. Upon manufacture the transmitter sends the initial seed code and key to the receiver to program the receiver (i.e. see Abstract). Therefore, it would have been obvious to a person of ordinary skill in the art at the time of the invention was made to include the algorithm generates the authenticator as a function of both the seed code and the function code of Gurney et al. as an alternative of decoding method of Brinkmeyer et al. in order to achieves same end result of allowing the operation of the vehicle system.

Referring to claim 4, Brinkmeyer et al. in view of Gurney et al. disclose the system of claim 3, Gurney et al. disclose wherein said portable unit transmits the enciphered specific key code to said vehicle-mounted control unit when a predetermined operation is conducted (i.e. See Abstract, col. 1 line 49 to col. 2 line 10; see Figures 2 and 5).

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Khamharn (US# 5,767,784) discloses the initialization method for keyless entry system.

Any inquiry concerning this communication or earlier communications form the examiner should be directed to Scott Au whose telephone number is (571) 272-3063. The examiner can normally be reached on Mon-Fri, 8:30AM – 5:00PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Michael Horabik can be reached at (571) 272-3068. The fax phone numbers for the organization where this application or proceeding is assigned are (571) 273-8300.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703)-305-3900.

Scott Au

SA
12/20/05

MICHAEL HORABIK
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2600